STATEMENT OF WORK

Defense Intelligence Agency Chief Information Office (CIO)
Enterprise Senior Information Technology Advisors III (ESITA III)

07 January 2022

Statement of Work (SOW)

Enterprise Senior Information Technology Advisors III
Unclassified
07 January 2022

GENERAL INFORMATION

This is a non-personal services contract to provide Enterprise Senior Information Technology Advisors Contract III (ESITA III) to the Defense Intelligence Agency (DIA), Office of the Chief Information Officer (CIO). The Government shall not exercise any supervision or control over the service contractors performing the services herein. Servicing contractors shall be accountable solely to the Contractor who, in turn is responsible to the Government.

1. Title of Project:

Enterprise Senior Information Technology Advisors (ESITA) III

2. Background:

The Defense Intelligence Agency (DIA), Chief information Officer (CIO) has seen significant growth in Information Technology (IT) thus increasing the need of expertise in cyber security, program management, technology and processes, acquisition and financial management, and organizational management. With this need came the establishment of a Blanket Purchase Agreement (BPA) of Enterprise Senior Information Technology Advisors (ESITA) Program. The basis for a BPA has allowed and will continue to allow CIO to obtain services to quickly address challenges that cannot be solved on typical IT support contracts. The CIO's Strategic Vision is to facilitate and enhance information sharing across the Defense Intelligence Enterprise (DIE), achieve world-class IT security and collaboration across multiple networks, and develop the CIO workforce to deliver these services efficiently and effectively. Additionally, CIO's focus is to strengthen its commitment to their customers through partnerships and collaboration, delivering consistent and reliable IT services helping the customer to achieve their program mission objectives.

3. Objectives:

The objective of this requirement is to establish BPAs that will allow CIO to quickly obtain expert level advisory and consultation support services. The services will ultimately enable the CIO to support warfighters, policymakers, and acquisition leaders across the DIE by achieving an information and communications technology advantage.

4. Scope:

ESITA services shall include a wide range of technical and non-technical activities to support IT security, engineering & operations, program management, administrative, financial, audit and contracting support services. Although functions and activities will crosscut the CIO and greater DIA organizations, ESITA services will be categorized into two lines of effort (1)

Cybersecurity Engineering and Technical Services and (2) Technical IT Consultation and Business of IT. Cybersecurity services aim at maintaining and improving the protection of network and communication's infrastructure and applications used by warfighters, policy makers, and acquisition leaders across the DIE. Technical IT Consultation will focus on providing technical advisory services for strategic, architectural, operation and implementation planning (less matters associated with Cybersecurity). The Business of IT will be the non-technical services that will enable the delivery of technology solutions or services.

ESITA support is akin to activities associated with System Engineering and Technical Assistance (SETA) such as but not limited to: deriving requirements, performing technology assessments, developing acquisition strategies, conducting risk assessments, developing cost estimates, determining specifications, evaluating contractor performance and conducting independent verification and validation, directing other contractors' (other than subcontractors) operations, developing test requirements and evaluating test data, and developing work statements. As advisors and consultants to the government, recommended courses of actions and solutions identified by ESITA support may be transitioned/transferred to other CIO contractor service providers to implement; transition/transfer of services to implement solutions is at the discretion of the government and will be assessed by the government on a case-by-case basis. Selected contractors shall have subject matter expertise and provide all resources necessary to perform the specific requirements.

5. Requirements

The ESITA contract vehicle streamlines the delivery and management, services, and functions for current and emerging requirements. Industry partners shall have relevant experience in essential services and the functions listed within this document. Government may require services for one to many of the functions listed. Enterprise activities and services may be combined to maximize efficiencies, drive process improvements, eliminate service overlaps, evolve with leading-edge processes, and realize cost efficiencies to provide strategic IT advantages to the US Government. The Contractor shall support activities in the following functional areas:

5.1. Cybersecurity Engineering and Technical Service

5.1.1. Provide ongoing cybersecurity engineering, architecture, and strategic planning services in support of DIA's transition to Zero Trust and a Data Centric Security Architecture. Continue to evolve DIA's Zero Trust Architecture transition by performing inventory of tools, processes, and data. Develop a phased plan that outlines parallel operations, and near-term focus areas such as Comply to Connect.

5.1.2. Develop transformation and modernization plans for Computer Network Defense (CND) capabilities on all classification domains. Responsible for consulting both internally and externally to provide technical expertise regarding the design, development, and implementation of complex security products and services utilizing Cloud services. Achieve cybersecurity data standardization by researching, analyzing, selecting/developing or adhering to DIA prescribed data standards.

5.1.3. Provide Risk Management Framework (RMF) guidance for all projects associated with JWICS Modernization.

5.1.4. Evolve and support the JWICS Cybersecurity Inspections Program (JCIP). Provide a mechanism for DIA to assess and report on the mission risk associated with JWICS subscribers and their enclaves to JWICS. Provide DIA and JWICS subscriber site leadership with key information to inform the cybersecurity decision process. Develop or identify, integrate, deploy, operate, and maintain automated tools in support of JCIP. Ensure all technical and evaluation data captured as part of JCIP is stored in a centralized location to enable ongoing data science and trend analysis activities.

5.1.5. Define, establish, automate, implement, execute, and enforce a comprehensive and mature Enterprise IT Asset Management (ITAM)plan and technical solution for the DIA Enterprise. Ensure organizational IT assets are accounted for, tracked, deployed, secured, maintained, upgraded, and disposed/replaced when end-of-life (EoL) is reached. Enterprise ITAM is foundational to the future implementation of zero trust architecture principals and automated Continuous Monitoring.

5.1.6. Conduct assessment activities, and assist in the expanded use of automated tools within the Risk Management Framework (RMF). Explore solutions for testing of source code and Secure Technical Implementation Guide (STIG) compliance. Determine areas for increased use of tools for continuous monitoring of the DIA IT Enterprise. Expand the Development Security Operations (DevSecOps) process and automated capabilities to additional application types and classification enclaves.

5.2. Technical IT Consultation and Business of IT

5.2.1. IT Engineering

5.2.1.1. Provide IT engineering consultant services associated with the infrastructure, applications, Tier III technical support, Special Access Programs (SAP), commercial cloud services, and hybrid hosting. Advise the government on planning and engineering services in support of information technology integration to include applications, data/data architecture, communications, infrastructure, systems, and storage. Integration may include design, planning, implementing, and testing. Engineering assistance will include planning, procuring, engineering, and architecture support at all phases of the IT life cycle

5.2.2. IT Operations

5.2.2.1. Advise the government on planning and engineering functions in support of (a) IT applications under the core services, messaging, business, and mission portfolios (b) data center planning and analysis and operations solutions (c) infrastructure management to include end-point management, communications, data storage and server operations (d) delivering and deploying IT products to the customer's workstation. IT Operations assistance will include planning, procuring, engineering, and architecture support at all phases of the IT life cycle.

5.2.3. IT Program and Project Management Support

5.2.3.1. Provide project management and planning services with the capability to manage IT projects of varying scope/size/complexity. Apply current project management best practices and frameworks such as but not limited to Project Management Institute (PMI) best practices (e.g., Project Management Body of Knowledge, (PMBOK), and any agency specific Software Development Life Cycle standards. Guide the development of project schedules, tasks, milestones, risks, alternative actions, within the context of a Risk Management Framework.

Monitor and intervene as needed in the implementation of project tasks in order to ensure the completion of project tasks, achievement of milestones and provision of deliverables on schedule and on budget (based on requirements). Support operations and maintenance for the IT applications/systems. Support existing processes and functions as well as needed changes across the entire life-cycle of the project. Support a wide range of financial, administrative, logistical, and management functions to meet program/project unique requirements.

5.2.4. Data Science

5.2.4.1. Collect, acquire, extract, integrate, inspect, clean, and model data from multiple sources, either new or existing. Analyzes and interprets data to discover trends and patterns toward resolving complex problems or managing initiatives and processes. Coordinates with organizations and stakeholders to identify holistic data-related strategies applicable to initiatives. Creates charts, dashboards, and presentations that effectively visualize analysis for effective decision-making. Manages data holdings and maintains information sites (e.g., SharePoint), ensures compliance with all applicable agency and organizational knowledge and data management guidelines and policies. Recommends data collection and analysis strategies for new projects.

5.2.5. Strategy

5.2.5.1. Provide guidance to CIO Offices for future IT strategy, policy, and planning guidance. Provide process, research, studies, analysis, drafting, and editing in developing the CIO Strategy, the CIO GDIP IT Planning Guidance (CPG), and other strategic-level documents.

5.2.5.2. Establish and refine a performance management framework such as a Balanced Scorecard approach, or any other framework approved by the Government. This support will include working across the CIO and mission partners to establish/refine a core set of outcome-based measures, measure targets, and current measure baselines for CIO that will demonstrate overall CIO organizational performance and health as well as identification of sub-metrics directly or indirectly supporting the overall outcome-based measures. These outcome-based measures and targets should be based on industry and government standards, best practices, and a history of success.

5.2.5.3. Support assigned special studies; participate in various special projects to meet unique customer requirements; identify future concerns, issues, and requirements; and develop strategies to accomplish project goals and requirements.

5.2.5.4. Identify, codify, and measure the progress of strategic initiatives that will drive the CIO organization towards successfully meeting its goals and objectives as stated in the CIO Strategy, DIA CIO IT General Defense Intelligence Planning Guidance (CPG) document, or other approved goals and objectives. Although not precluded, this support does not necessarily include the execution of any initiative.

5.2.5.5. Identify and assess innovative technologies, evaluate industry best practices and explore the methods to integrate emerging technologies into the DIA IT enterprise. Advise and assist the government in developing technology strategies for the CIO and Intelligence Community for both the near and long term.

5.2.6. Program Administration

5.2.6.1. Provide administrative support and guidance to CIO Offices for the full range of training, career development, and succession management programs. This task includes cultivating and providing an environment for continuous learning, using the right skills at the right time, promoting career mobility, acquiring the right balance of civilian, military, and contractor professionals, and personnel integration. Task also includes succession program implementation to achieve and execute a successful succession management strategy.

5.2.6.2. Establish and/or maintain a directorate level records management program to adhere to the Agency's and DOD's record management statues. Create and deliver a project plan including identification of tools and methodologies to execute a directorate records and data survey project; execute a records and data survey, including personal interviews across the directorate; draft records and data retention schedules; and create and/or revise the directorate file plan and taxonomy, including supporting procedures and guidelines.

5.2.7. Communications

5.2.7.1. Provide leadership in the identification, crafting, and execution of strategic narratives to the organization's stakeholders. Implement organizational change management methodologies tailored to the scope of initiatives across CIO to drive adoption of IT changes. Develop, update, and maintain multiple website sites across multiple platforms. Produce graphics, videos, slick sheets, briefing materials, logos, and various CIO documents for CIO communications. Support virtual and in-person event planning and execution, including potential virtual CIO events and conferences. Plan, coordinate, produce, review, and edit content of material publication. Assess current Government customer relationship and experience programs via customer surveys, policy review, interviews, focus groups and product reviews.

5.2.8. Customer Engagement

5.2.8.1. Assess current Government customer relationship and experience programs via customer surveys, policy review, interviews, focus groups and product reviews. Refine or enhance a requirements management function that improves the customer experience by providing a single point of contact for all requirement types. Provide services that will ensure improved visibility and optimization of constrained resources, and reduce risk by ensuring all work is prioritized, sponsored and resourced for success. Work with customers to clarify their needs, developing functional requirements documents, collaborating with stakeholders to help establish priorities, and support continuous process improvement functions. Perform metrics development, root cause analysis and process improvement employing techniques to improve the

effectiveness and efficiency of CIO processes. Identify candidate processes for improvement and assist in executing process improvement projects.

5.2.9. Business Operations and Governance

5.2.9.1. Provides various pre and post award acquisition support functions relating to contract management, and program management support. Establishes processes and procedures for properly vetting acquisition requirements including enhancing acquisition governance policies, facilitating working groups, and maturing acquisition documents. Provides acquisition planning, requirements definition, and performance monitoring support. Supports the development of Program Management Plans, Market Research documents, Requirements documents and Source selection plans. Establish and implement program governance criteria and oversight on multiple award, multiple task order efforts. Prepare, maintain and implement acquisition plans and various administrative functions to include program control and tracking.

5.2.9.2. Perform various contract preparation, administration and contract management responsibilities from origination to termination of the acquisition process. Engage in acquisition planning, Request for Proposal/Invitation for Bid preparation, and source selection process. Assists the Contracting officer during the acquisition planning and source selection process. Develops customer needs statements, Requests for Information, Requests for Quotes. Administer contract terms and conditions, preparation of contract modifications, contract termination, and contract closeout.

5.2.9.3. Provide governance and oversight relating to acquisition, contract management, and program management. Develop, maintain and utilize data collection methodologies to assess contract performance against strategic, operational, and tactical objectives. Monitor and intervene as needed regarding contract staffing and expenditure levels during period of performance. Produce, monitor and oversee financial data input/output reporting. Provides summary data as requested in the form of ad-hoc and scheduled quarterly and monthly reports.

5.2.9.4. Perform functions to support CIO corporate decision-making processes such as implementing and administering the CIO Integrated Governance Framework and the Intelligence Planning, Programming, Budgeting, and Evaluation process. Identify alternatives and provide recommendations to reduce costs and improve financial performance.

5.2.9.5. Perform financial management and resource allocation functions acquisition planning and programming, budget and execution. Develop, implement and monitor plans for monetary spending, resource allocation, execution of resources and financial justifications. Provide program management, business, and technical support to drive the planning and implementation of required objectives and programs. Provide expertise and best practices to optimize business spending to deliver on business and mission priorities.

5.2.10. Internal Controls and Auditing

5.2.10.1. Provide IT audit support to ensure internal controls are working effectively across the agency. Support services include but are not limited to the following: assist in detecting and preventing fraud, waste, or abuse of IT services, assist in understanding the general risk faced and the impact of those within the organization, collect information and documentation that may be treated as evidence, assist in understanding customer's internal control strengths and weaknesses, assist with evaluating compliance and ethics programs, work to summarize, analyze and prepare analysis reports and findings clearly and concisely, where required, assess the information assurance (IA) posture of information systems and networks, to include new technologies, e.g., new operating systems, the capabilities and optimum application of IA tools, to include firewalls, intrusion detection systems, information assurance vulnerability alert (IAVA) management tools, scanners, and other technologies.

6. Deliverables

Deliverable	CDRL	Description	Quantity/Media	Due Date
Transition and Integration Plan	A0001	provide a plan that describes how it will assume responsibility for human capital to include Contractor's transition and integration	e.g., five (5) printed copies and three (3) copies on CD-ROM	plan (not to exceed 90 days from award) to seamlessly assume and perform the full range of all work processes and services
Administrative-Related Deliverables	A0002	deliverables will be submitted electronically on the CIO-5 STORMS SharePoint Portal		TBD
Weekly Activity Report (WAR)	A0003	keyed to tasks for each Order accomplished submitted in soft copy format by the contractor (CO and COR only).	e.g. five (5) printed copies and three (3) copies on CD-ROM	Weekly submission Day (TBD) To be determined timeframe

Monthly Contractor Activity Status Report (CAR)-	A0004	program/ cost information. Additional sections or details subject to change upon request. contract/order number/brief functional description reporting period. staffing status, vacancies and number of days the positions have been vacant, monthly costs, deliverables, summary of key activities accomplished, and any significant issues, risks, problems and resolution. written progress reports monthly for the period for entire contract period or project duration. The original and 3 copies are required. identify any problems that arose and a statement explaining how the problem was resolved. identify any problems that have arisen but have not been completely resolved and provide an explanation.		Monthly (TBD) To be determined timeframe.
Close-Out Report	A0005	To include customer input all up-to-date what the customer analyses of essential information needed to sustain operations after order expiration. The report shall include all Government owned property, inventories, Government owned software, etc.		End of the order base POP year or current option year.

Expense Report	A0006	Provided monthly in a government provided template: invoice details by contract, order, contract line-item number, subcontract line-item number, ACRN, resource, labor category, hours, negotiated rates, and billing amounts.		Monthly (TBD) To be determined timeframe.
Quarterly Business Review (QBR) Brief	A0007	brief conducted once every quarter. Providing information regarding cost, schedule, performance a nd risk of the order shall be completed with Government provided template		This brief will be completed once every quarter.
Contractor Auditor Detail Activity Report (CADAR)	A0008	Include, but is not limited to negotiated rates, and billing amounts. activity report which includes expenses, hours to contract number, contract line-item number (CLIN), subcontract line-item number, invoice details, ACRN, resource, labor category, hours,	The report shall be submitted to the COR via EMAIL.	Monthly, report submitted to COR no later than 4:00 PM on the 30th day of each month.
Transition Report	A0009	contractor will work with the COR to identify what information is to be included in the transition plan. the Contractor is required to provide training on the business process and/or system to the government personnel identified by the COR and if applicable, the successor Contractor to avoid interruption in service.		No later than 120 days, prior to the expiration of the contract/Task Order/Delivery Order. shall be submitted electr onically to the COR no later than 4:00PM on the 28th day and 60 days prior to the month of expiration of the contract.

Onsite Contact	A0010	POC who can leverage and communicate with the government contact/PM to quickly respond to changing /evolving mission needs as they occur.		Daily, Weekly or upon request.

6.1. Transition and Integration Plan- Contractor to provide a plan that describes how it will assume responsibility for all human capital work detailed in this statement of work to include Contractor's transition and integration plan (not to exceed 90 days from award) to seamlessly assume and perform the full range of all work processes and services described in the statement of work.

6.2. Administrative-Related Deliverables- All administrative-related deliverables will be submitted electronically on the CIO-5 STORMS SharePoint Portal and will follow Government standards to include, but not limited to format, structure, templates, and timelines unless otherwise requested by Government officials.

6.3. Weekly Activity Report- A weekly activity report (WAR), keyed to tasks for each Order accomplished during the weekly determined timeframe, will be submitted in soft copy format by the contractor (CO and COR or government appointed personnel only).

6.4. Monthly Contractor Activity Status Report (CAR)- Monthly status reports shall contain all program and cost information and will follow the Government provided template. Additional sections or details can be requested at Government request. The format report shall include the contract and order number, a brief functional description, and the reporting period. It shall also contain staffing status to include all vacancies and the number of days the positions have been vacant, monthly costs, deliverables, a summary of key activities accomplished, and any significant issues, risks, problems, and resolution.

6.5. Close-Out Report- Working with the COR, at the end of the order base year or current option year, the Contractor shall provide a close-out report. The close-out report shall include customer input such that all up to date what the customer concedes is essential information needed to sustain operations after the order expires. The close out report shall include all Government owned property, inventories, Government owned software, etc.

6.6. Expense Report- The expense report will be provided to the Government monthly and will follow the Government provided template. Includes, but is not limited to invoice details by contract, order, contract line-item number, subcontract line-item number, ACRN, resource, labor category, hours, negotiated rates, and billing amounts.

6.7. Quarterly Business Review (QBR) Brief- This brief will be completed once every quarter and briefed at the QBR meeting. It details information regarding cost, schedule, performance, and risk of the order and will follow a Government provided template.

6.8. Contractor Activity Report -The Contractor shall provide a monthly activity report which includes expenses, hours, and the items listed. The report shall include, but is not limited to contract number, contract line item number (CLIN), subcontract line item number, invoice details, ACRN, resource, labor category, hours, negotiated rates, and billing amounts. The report shall be submitted to the COR no later than 4:00 PM on the 30th day of each month.

6.9. Transition Plan - The contractor will work with the COR to identify what information is to be included in the transition plan no later than 120 days prior to the expiration of the contract/Task Order/Delivery Order. The plan shall be submitted electronically to the COR no later than 4:00PM on the 28th day and 60 days prior to the month of expiration the contract. In addition, prior to the expiration of the contract, the Contractor is required to provide training on the business process and/or system to the government personnel identified by the COR and if applicable, the successor Contractor to avoid interruption in service. The transition period should be no longer than sixty (60) days.

7. Place of Performance

7.1. As the Government requirements programs matures, reallocation of contract support to various government and contractor hosted locations may become necessary.

7.2. The place of performance will be at DIA enterprise sites that will include, but are not limited to the locations listed below

- National Capital Region (District of Columbia, Quantico and Reston Virginia, College Park, Maryland)
- Norfolk, VA
- Colorado Springs, CO
- Tampa, FL
- Charlottesville, VA
- Pearl Harbor, HI
- Makalapa, HI
- Miami, FL
- Scott AFB, IL
- Offutt AFB, NE
- Seoul, South Korea
- Stuttgart, Germany

7.3. Cyber SCIF and Place of Performance requirement

7.3.1. Contractor Facilities - SCIF(s). The Government intends to sponsor contractor hosted SCIF(s) within the National Capital Region (NCR) in order to provide the services described in this SOW for cyber related requirements. For a number of services provided within the NCR, the contractor SCIF may be the primary work location based on space availability and requirements at Government facilities. Any facilities supporting the ESITA contract shall have proper SCIF with

sufficient capacity to support the cybersecurity requirements defined in this SOW.

7.3.2. The contractor must either already have their own SCIF, or be able to stand up a SCIF, within 180 days of award. The SCIF accreditation (TS/SCI) be in accordance with ICD 705 and have adequate bandwidth with fully reliable connectivity to the governments classified and unclassified network infrastructure. The contractor shall provide Government access rights to their SCIF. Access shall be granted to personnel approved by the Government. This includes scheduled and periodic service/SCIF audits, inventory, and inspections. The Government retains the right to evaluate and approve these SCIFs.

7.3.3. The Contractor shall be responsible to comply with all SCIF requirements and standards for maintaining, securing, and operating classified IT systems. This includes, but is not limited to, Security Technical Implementation Guidelines (STIGs), Information Assurance Vulnerability Management (IAVM), Intelligence Community Vulnerability Management (ICVM), security auditing and monitoring and provision of security log data, FISMA, and all applicable DOD and DIA requirements.

7.3.4. The Government shall be given access rights to the ESITA SCIFs. Access shall be granted to personnel approved by the Government, provided that a specific NDA has been accepted by the ESITA Contractor, for scheduled and periodic service/SCIF audits and inspections.

7.3.5. The contractor shall maintain physical security of ESITA assets to prevent the loss of data, software and hardware (e.g., physical access, etc.). Access to ESITA assets is for ESITA staff and government officials who are authorized by the Contracting Officer or a Project Manager.

8. Telework

8.1. Telework and flex of duty days is authorized if approved by the Government Contracting Officer; all request must be submitted to the COR.

9. Government Furnished Property, Material, Equipment, or Information (GFP, GFM, GFE, or GFI).

9.1. The Government will provide contractor employees with the following property at their assigned work locations as needed:

9.2. Access to Non-Secure Internet Protocol Network (NIPRNet), Secure Internet Protocol Network (SIPRNet), and the Joint Worldwide Intelligence Communications System (JWICS) networks and systems access, including printers and digital senders.

9.3. Contractor employee use of DoD Computers is FOR OFFICIAL USE ONLY and its use is subject to monitoring at any time. All data generated or collected on DIA computers becomes the property of the U.S. Government and its release, downloading or transmittal is subject to Government approval. Contractor personnel are not authorized to introduce computer hardware,

software, or data storage media; physically or electronically; into a Government facility, computer, or network device without the prior written approval and notification of the appropriate Government authorities. Downloading and transmitting of information within DIA's custody is prohibited except as provided for in the terms of this contract.

10. Duty Hours

10.1. Duty Hours- Continental United States (CONUS)- The core work hours of operations for all personnel assigned within the National Capitol Region (NCR) are Monday through Friday (0600 – 1800) hours. A 40-hour workweek is anticipated for the contractor personnel; however, the week may be extended to meet operational needs with prior, written, COR approval. The Program Manager shall obtain COR approval, in writing, prior to any performance more than 40 hours per week to ensure availability of funding.

10.2. Duty Hours- Overseas Continental United States (OCONUS)- Contractor employees supporting OCONUS contingency operations shall work twelve (12) hours per day, seven (7) days per week, and eighty-four (84) hours per week from Monday through Sunday (i.e., Afghanistan). In non-contingency locations (i.e., Cambodia), contractor employees shall work eight (8) hours per day, five (5) days per week, and forty (40) hours per week from Monday through Friday. Contractor personnel shall not exceed the designated work weeks without prior, written, COR approval.

10.3. Duty Hours- Combatant Commands (CCMD)- Contractor personnel assigned to Combatant Commands (CCMD) and other national agencies outside of the NCR must adhere to the supported headquarters core hours at their assigned location.

10.4. The contractor is responsible for conducting business, between the hours approved by the organization and the COR Monday through Friday; except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings

10.5. Overtime will be managed on a case-by-case basis and requires pre-approval from the Government. In the occurrence of an unplanned emergency, the Contracting Officer shall be informed immediately.

10.6. Surge Requirements. N/A

11. Travel

11.1. If travel becomes necessary to support this contract's program, the government will reimburse travel expenses IAW the guidelines in the Joint Travel Regulations (JTR). Local travel within a fifty-mile radius of DIA HQs, contractor work locations is non-reimbursable to the contractor unless otherwise agreed by the Contracting Officer. All travel shall be approved in writing by the COR prior to making any reservations. Contractors shall consult the Defense Travel Management Office website (www.defensetravel.dod.mil) prior to traveling to obtain

updated per diem rates for the locality to which they are traveling. Travel and Per Diem Rates (2021).

11.2. Local travel, within 50 miles of duty location, will not be reimbursed. The principle place of performance in the Washington, DC National Capital Region (NCR) with primary work location at DIA Headquarters, Reston 1, 2, and 3, MS2, Indian Head, MD, and Quantico, Virginia. Tampa, FL and Colorado Springs, CO are also possible principle places of performance. Accordingly, reimbursable travel and per diem for the contractor's employees performing work on a regular basis at this place of performance is not authorized.

12. Security Requirements

12.1. The DIA has determined that performance of this contract requires that the Contractor, subcontractor(s), vendor(s), etc. (herein known as Contractor), requires access to sensitive DIA information, the Contractor shall have a facility clearance, and that the Contractor will adhere to the following:

12.2. All level of effort employees shall have an active TOP SECRET clearance and be eligible to access to Sensitive Compartmented Information (SCI). No contractor individual will be accepted whose Single Scope Background Investigation is four (4) years or older. Physical security, document security, and electronic media security will follow the Defense Industrial Security Regulations.

12.3. The Computer Security Act of 1987, Federal Information Security Management Act (FISMA) of 2002 and the DIA Instruction 85000.001, "DoD SCI and DoDIIS Community Information Assurance (IA) Program," mandate that all DoD civilian, military, and contractor employees with access to government information technology systems must complete annual IA Awareness training. All contractor employees using DIA's automated system or processing Agency's sensitive data will be required to complete the annual IA Awareness training.

12.4. The contractor shall ensure that all contractor personnel performing work at a DIA work site and/or requiring access to DIA networks shall accurately enter and maintain required personal, administrative, and career information in DIA's official human capital management system myHR as described in DIAI 1700.001 and other DIA business process documents. Information maintained in myHR is protected by the Privacy Act of 1074. DIA will use this 1700.001 and other DIA business process documents. Information maintained in myHR is protected by the Privacy Act of 1074. DIA will use this information to facilitate enterprise management and operations. Contractor personnel are required to understand what data they are responsible for maintaining and update their myHR records within 72 hours after an event occurs that requires a record update.

12.5. DIA's Privacy Act Program: DIAI 5400.001 applies also to Federal contractors when the contractor will design, develop, or operate a system of records on individuals to accomplish an agency function. Violations of the Act may involve the imposition of criminal penalties.

12.6. The Contractor shall adhere to all local security procedures required by the Government, as well as the security procedures dictated in DD Form 254, DoD Security Classification Specification when on Government property. This program is classified UNCLASSIFIED.

12.7. A special provision exists regarding security clearances and access to Sensitive Compartmented Information (SCI). The contractor shall provide sufficient personnel (project manager) with Top Secret security clearances and SCI accesses to permit planning, management, development, and coordination as may be appropriate.

12.8. Classification Markings Adherence. The Contractor shall properly mark all materials and course content by adhering to the Classification Markings specifications as indicated in the "Intelligence Community Classification and Control Markings Implementation Manual" (Version: 20070328) issued by the Director of National Intelligence (DNI) Special Security Center (SSC), Controlled Access Program Coordination Office (CAPCO).

12.9. See DD Form 254 for Security Guidance.

13. Information Security.

13.1. All persons performing work under this contract shall protect and safeguard information in accordance with DoD, (as applicable) and DIA directives, instructions, and procedures. These same persons shall immediately report any deviation or violation of this guidance, or any unusual or suspicious activity to the DIA Security Office. These same persons will provide assistance and full cooperation in any subsequent investigations or inquiries conducted by DIA or other governmental agencies.

14. Annual Training.

14.1. Contractors are required to take all DIA mandatory training.

15. Non-Disclosure Requirements (NDA).

15.1. The Contractor shall have all personnel assigned to this contract complete a non-disclosure agreement (NDA) with copies provided to the COR. The NDAs shall not include any wording allowing the contractor to keep copies of proprietary information beyond the life of the contract. All estimates performed, models and model interfaces developed, and data collected under this contract are the sole property of the Government. All contractor personnel shall sign, prior to beginning performance, a non-disclosure agreement in accordance with DFARS 227.7103-7 and/or a DSS Non-Disclosure agreement. The Contractor is bound by all NDAs signed by its employees. In the event a contractor employee violates any of the terms of the NDA, the Contractor will be considered in breach of contract. This could result in a termination for default.